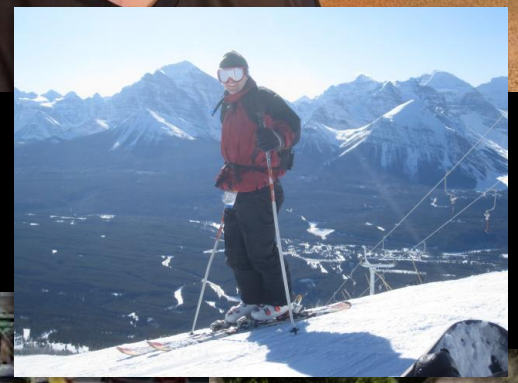
Ghosts in the Machines
Secrets of Cyber and AI

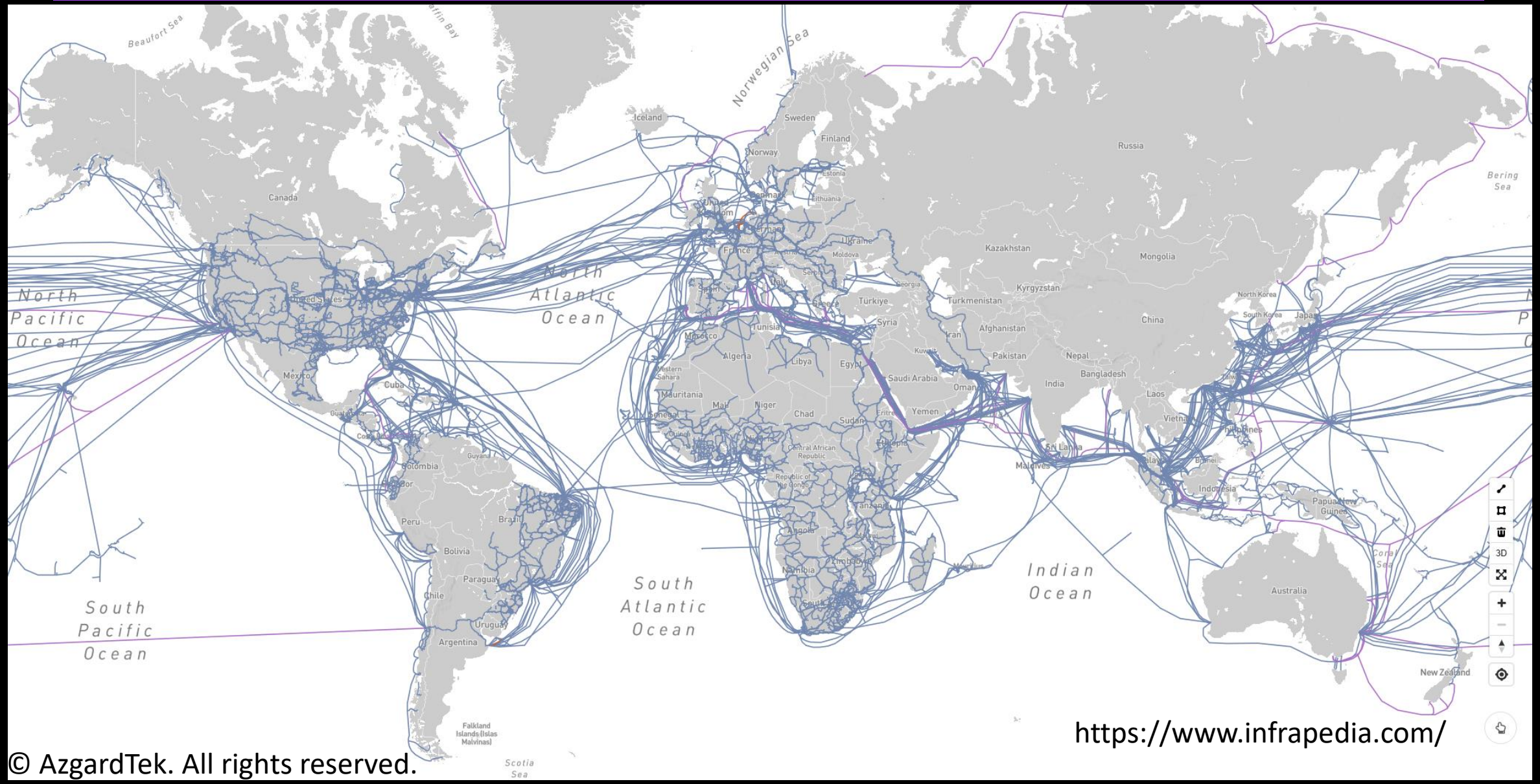
Julian Zottl
CTO, AzgardTek
https://www.linkedin.com/in/julianzottl

Intro

- **Past**
  - Programming in BASIC in 2nd grade, C by 4th
  - Undergrad and Masters in Electrical Engineering
  - Past - Vitreous State Lab -> NASA -> FannieMae ->
    Raytheon (18 years) -> NightWing (9 mo)
  - Chief Architect on Nation State Systems, the USG Protection System, etc.
- **Present**
  - Chief Technology Officer, AzgardTek
  - Cyber and Information Operations (IO) Subject Matter Expert (SME)
  - Multiple patents
  - Red Teamer National Collegiate Cyber Defense Competition, Sr. Mentor
    US Cyber Team, STEM outreach and presentations
  - MIT board for Generative AI and Machine Learning
  - Board of Advisors for Walacor
- **Personal**
  - Track, rallycross, skiing and climbing



The Play/Battleground

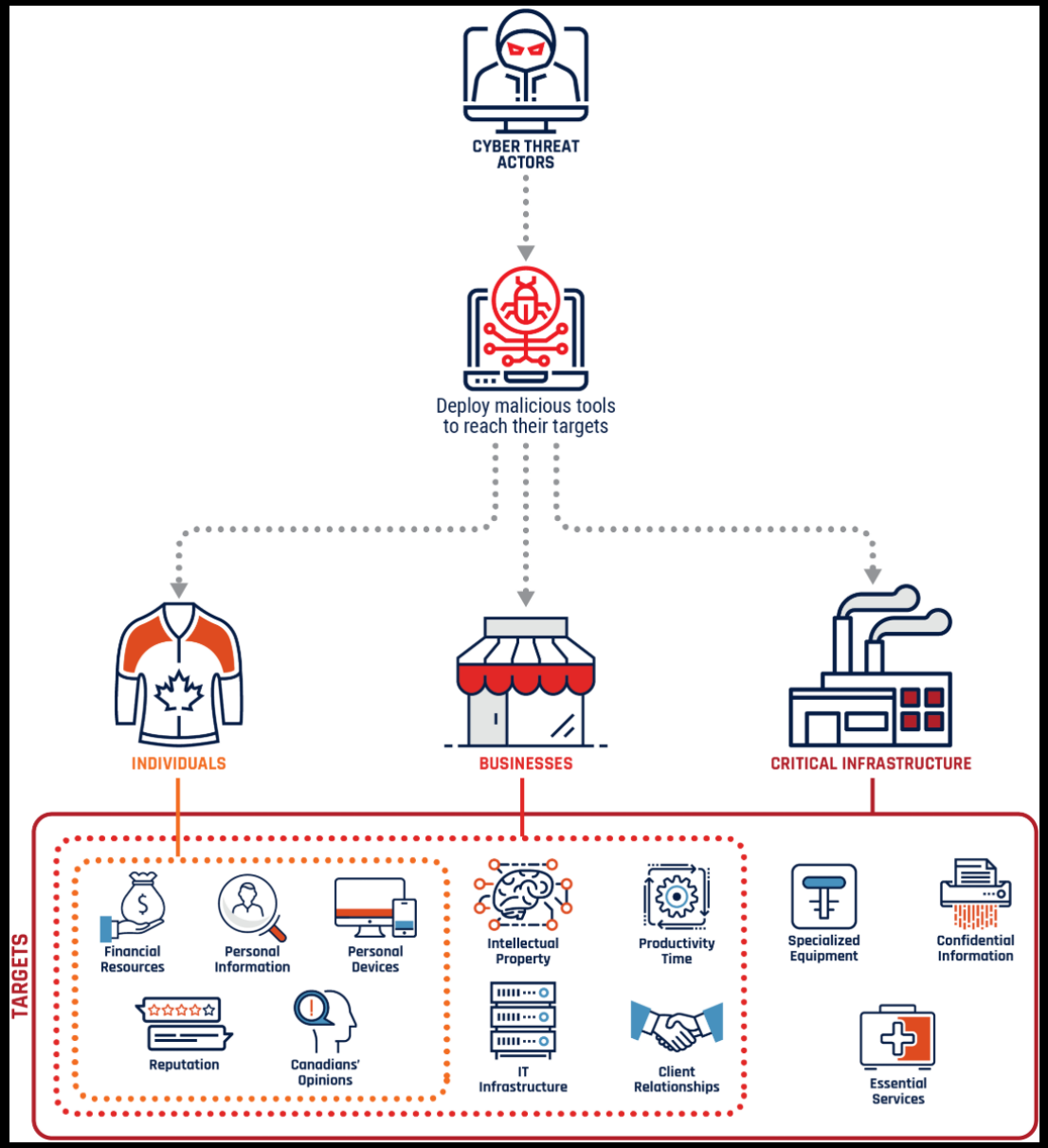


https://www.infrapedia.com/

Background Noise

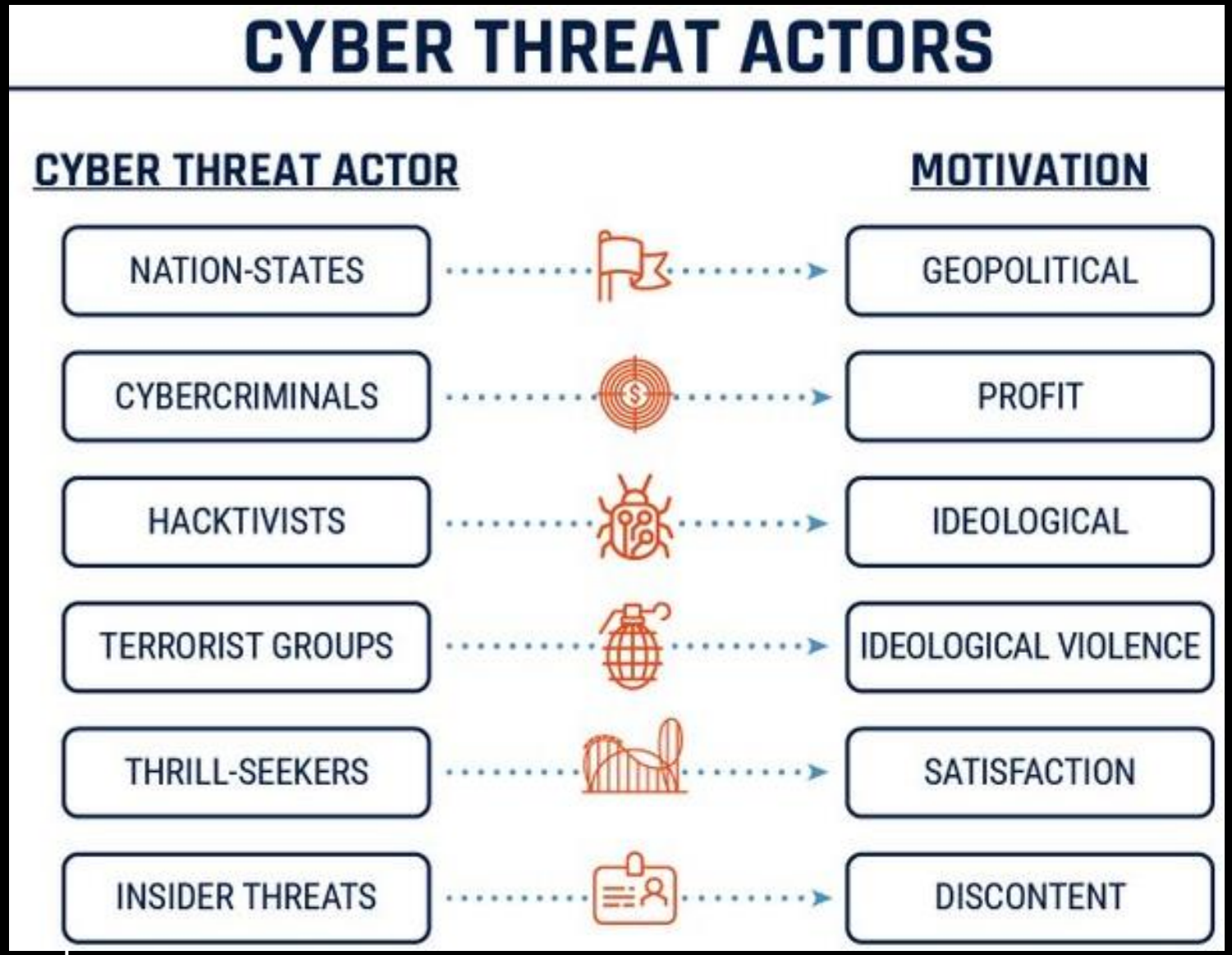
https://www.domo.com/learn/infographic/

Targeting and Motivation



https://www.cyber.gc.ca/en/guidance/

Motivation



https://www.cyber.gc.ca/en/guidance/

Three Major Cyber Threat Actors: China

- Motivations
  - Long-term strategic competition; accelerate technological development; gain military, economic, and political advantage; reinforce domestic control and influence abroad.
- Capabilities
  - Highly resourced state-sponsored units (PLA/Ministry of State Security); advanced persistent threats (APTs) capable of zero-day exploitation, supply-chain compromises, and large-scale espionage campaigns.
- Targets
  - U.S. government and defense contractors, critical infrastructure, semiconductor and biotech sectors, AI/quantum research, and diaspora communities.
- Tactics
  - Cyber-enabled intellectual property theft, strategic data exfiltration (e.g., OPM, Equifax), persistent access for wartime contingency planning, and disinformation to shape global narratives.

Three Major Cyber Threat Actors: Russia

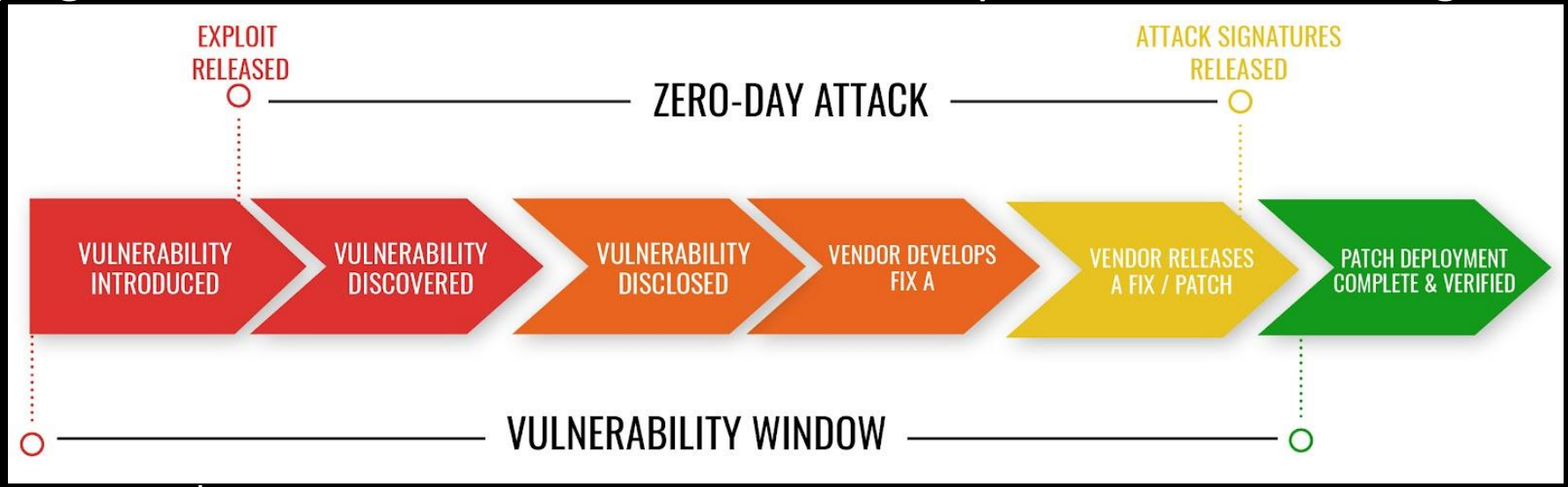
- Motivations
  - Undermine Western unity; destabilize adversaries politically and socially; maintain strategic influence in post-Soviet regions; project global power despite economic constraints.
- Capabilities
  - Well-established offensive cyber units (GRU, SVR, FSB); proven ability to conduct disruptive and destructive operations (e.g., NotPetya, Ukraine grid attacks) alongside sophisticated espionage.
- Targets
  - Energy, financial, and government sectors in NATO countries; Ukraine's critical infrastructure; international organizations (EU, UN); political parties and election systems.
- Tactics
  - Coordinated influence operations (state media + cyber), wiper malware and ICS/SCADA sabotage, false-flag intrusions to obfuscate attribution, long-term espionage campaigns.

Three Major Cyber Threat Actors: Iran

- Motivations
  - Regional influence and regime survival; deterrence and retaliation against Western sanctions or perceived threats; bolster asymmetric warfare capacity.
- Capabilities
  - Less sophisticated than China/Russia but improving; Islamic Revolutionary Guard Corps (IRGC) aligned groups with ransomware, DDoS, and wiper malware capabilities. Known for opportunistic but persistent APT activity.
- Targets
  - U.S., Israel, Gulf states' energy sectors, dissidents abroad, shipping/maritime industry, and regional critical infrastructure.
- Tactics
  - Website defacements, spear phishing, destructive malware (e.g., Shamoon variants), ransomware campaigns for both revenue and disruption, and coordinated cyber + kinetic attacks (e.g., against regional adversaries).

Some Stats

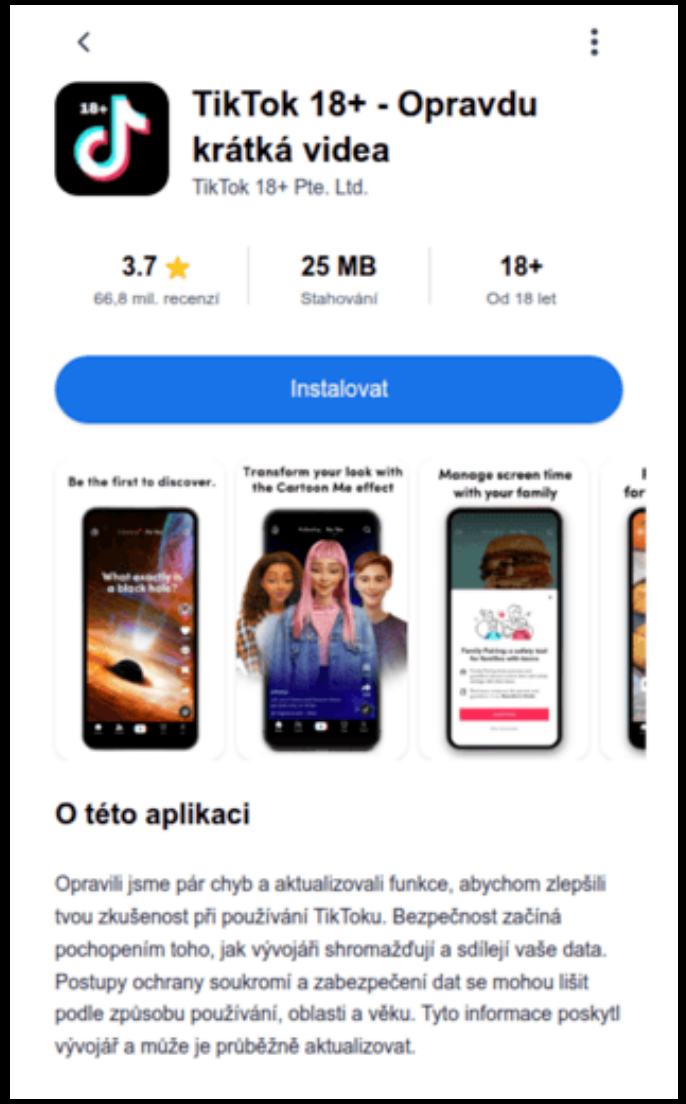
- For the Year as of Aug 2025
  - 4,562 zero-day vulnerabilities, ~570 discoveries per month
- DDoS attacks surged by 41% in 2024
- Vulnerabilities like CVE-2024-5806 “MOVEit Transfer” were exploited within hours of disclosure
  - Speed of weaponizing CVE’s has increased exponentially with the advent of AI
- Deploying Zero Trust methods has saved $1.76M per breach on average



https://mixmode.ai/blog/zero-day-attack-strategy/

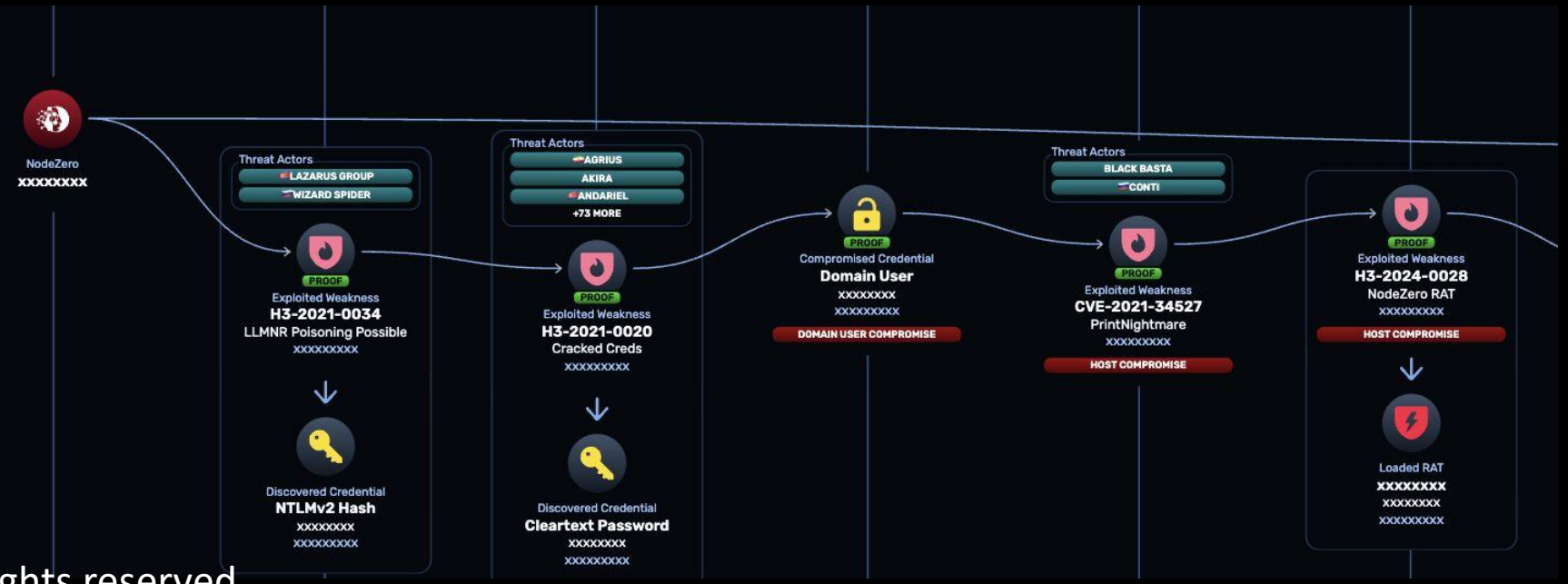
Example of 2025 Breaches

- RatOn: Android Banking Trojan
  - Written from scratch
  - Spreads via adult themed websites (TikTok18+) as an “installer”
  - Installs NFSkate – Skims card data via NFC
  - Grabs PINs and automatically executes unauthorized transfers
- Google’s Salesforce Data Breach
  - Asks 2.5B Users to Update their Passwords and use 2FA
- 16B Passwords Exposed
  - Usernames, passwords, tokens, cookies, and metadata
  - 30 separate datasets inc. Facebook, Google, Apple, GitHub, and Telegram

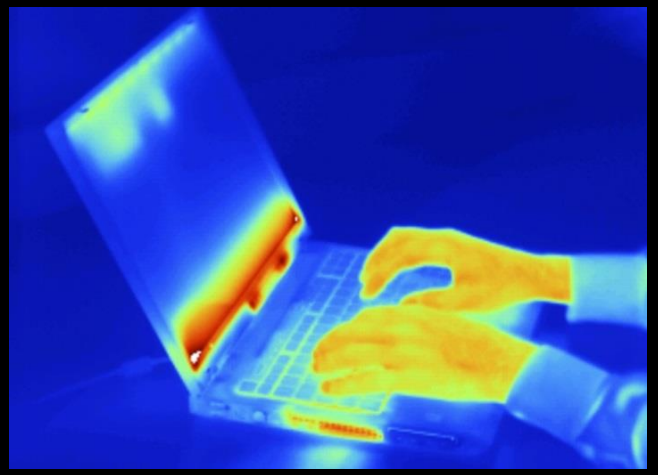


Example of 2025 Breaches

- Slack Workspace (October 2025)
  - No humans involved in this attack, it was fully autonomous via NodeZero
  - No prior knowledge of the environment or specific pre-training
  - No LLMs required, this attack required standard NodeZero graph analytics / "Next Best Action" techniques
  - This was run against an actual production network, not a lab
  - Compromised Rapid7 service account -> Exploiting a misconfigured SentinelOne Agent -> Accessing Slack authentication token -> Gaining access to the Slack workspace



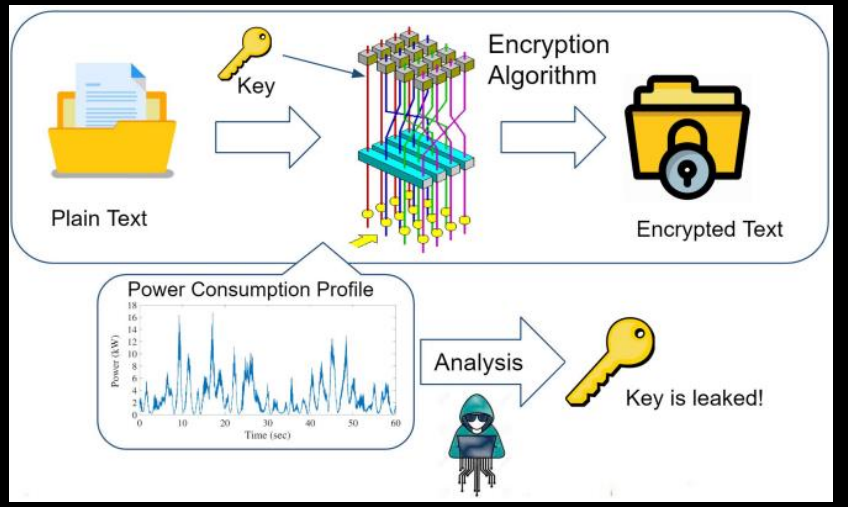
Side Channel Attacks – Electro, Magnetic, Sound, and Power

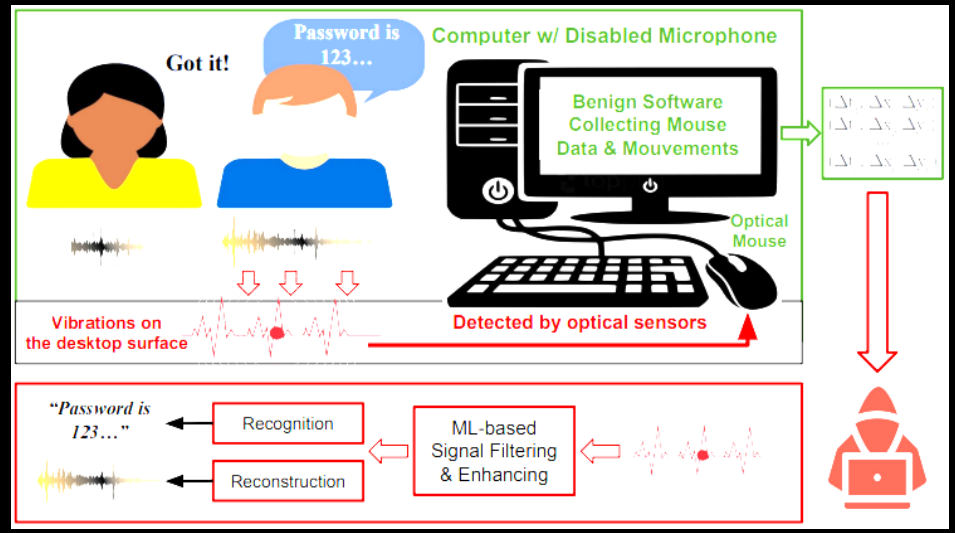


- **Optical Leakage** - Leakage of Information via LED's – (2002)
- **Cold Boot** - Attacking RAM for Private Keys – (2010)
- **BadBIOS** - Propagating via Sound – (2013)
  - Check: https://smus.com/ultrasonic-networking/
- **BitWhisper** - Using Thermals to Export Data – (2014)
- **GSMem** - Internal Buses to Transmit at Cellular Frequencies – (2015)
- **RowHammer** – Changing Memory in Adjacent Locations (2016)
- **DiskFiltration** - Data Exfiltration via Covert Hard Drive Noise (2016)
- **WindTalker** - Sniffs a user's fingers movement on the phone's touchscreen or a computer's keyboard by reading the radio signal patterns called Channel State Information (CSI). CSI is part of the WiFi protocol which provides general information about the status of the WiFi signal. (2016)

Side Channel Attacks – Electro, Magnetic, Sound, and Power

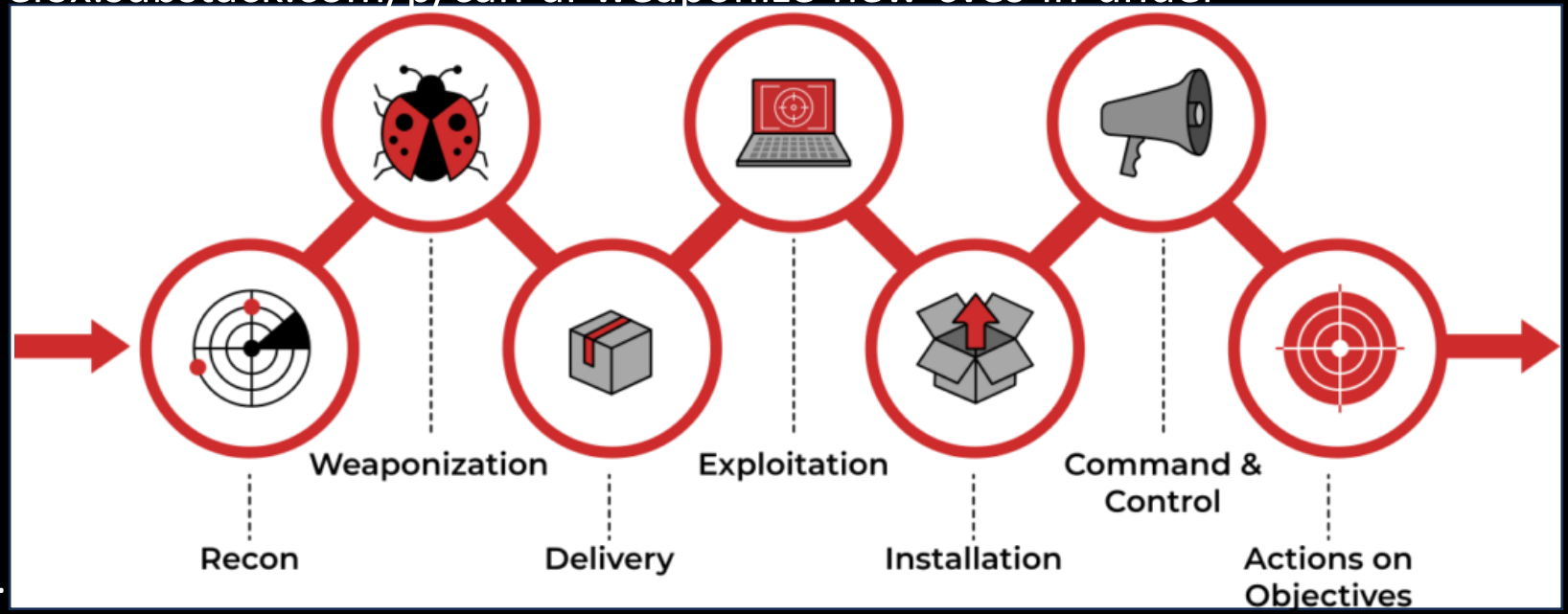
- **Differential Power Analysis** – Extraction of AES keys via powerline (20xx)
- **Collide+Power** – (2023)
  - 1st: Measures CPU power consumption over thousands of iterations while changing the data that can be controlled in shared memory. Enables the attacker to determine the data associated with the user applications, such as passwords or encryption keys.
  - 2nd: Attacker exploits a prefetch gadget within the operating system. This prefetch gadget can be used to bring arbitrary data into the shared CPU component and force data collisions to recover the data.
- Mic-E-Mouse - Use the sensors in optical mice to capture subtle vibrations and convert them into audible data (2025)





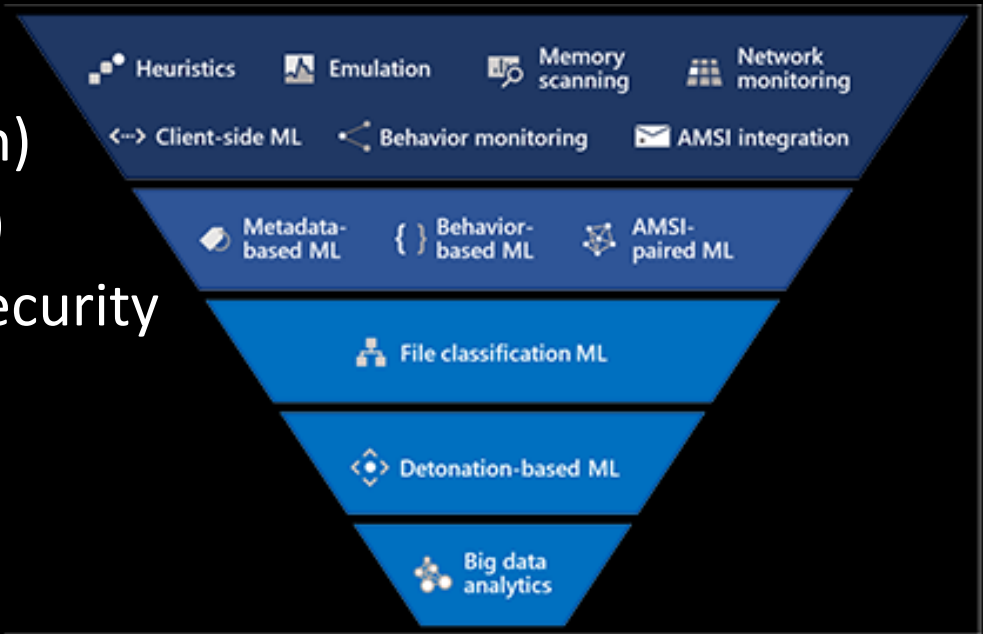
What about this AI thing?

- Offensive Cyber
  - AI is being used for all phases of the Cyber Kill Chain
  - https://autoexploit.ai/ - Generates exploits for new vulnerabilities in under 10 minutes for $1
  - https://valmarelox.substack.com/p/can-ai-weaponize-new-cves-in-under

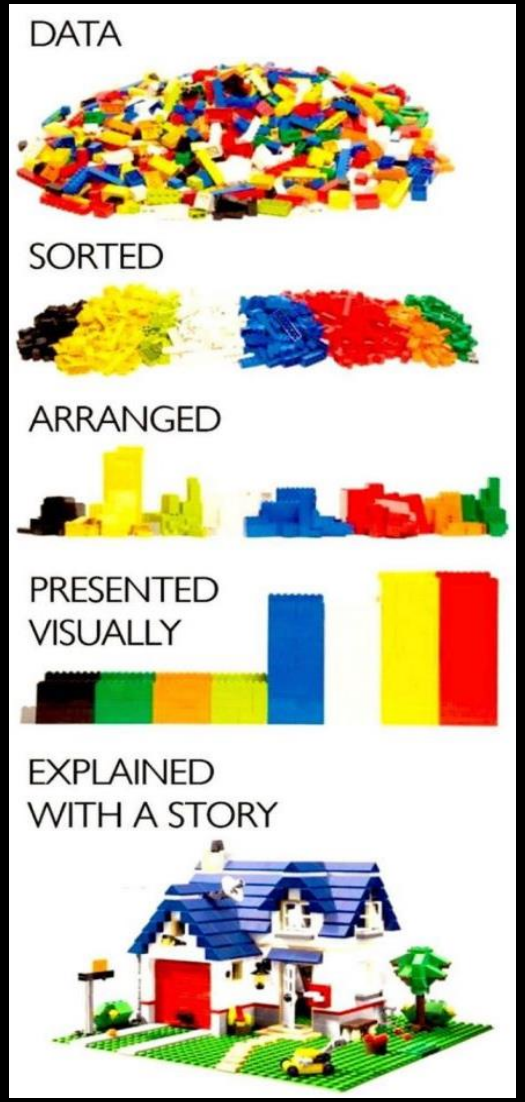


What about this AI thing?

- Defensive Cyber
  - Lagging in AI automation (not a technical reason)
  - Platforms using AI (Everyone had AI at Blackhat)
  - Need standards for cross AI collaboration and security



- Future of Defensive Cyber
  - AI will replace the Security Operations Center
  - Incorporating data from the physical world, hardware, operating system, data, user, network, business logic, threat feeds, etc.
  - Internal and external AI from “trusted” partners will collaborate
  - Threat Intelligence will become predictive



THANK YOU

If you liked this presentation, reach out and I can give it at your organization!
jzottl@azgardtek.com

Backup

Updated Password Table

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	57 minutes	2 hours	4 hours
6	Instantly	46 minutes	2 days	6 days	2 weeks
7	Instantly	20 hours	4 months	1 year	2 years
8	Instantly	3 weeks	15 years	62 years	164 years
9	2 hours	2 years	791 years	3k years	11k years
10	1 day	40 years	41k years	238k years	803k years
11	1 weeks	1k years	2m years	14m years	56m years
12	3 months	27k years	111m years	917m years	3bn years
13	3 years	705k years	5bn years	56bn years	275bn years
14	28 years	18m years	300bn years	3tn years	19tn years
15	284 years	477m years	15tn years	218tn years	1qd years
16	2k years	12bn years	812tn years	13qd years	94qd years
17	28k years	322bn years	42qd years	840qd years	6qn years
18	284k years	8tn years	2qn years	52qn years	463qn years

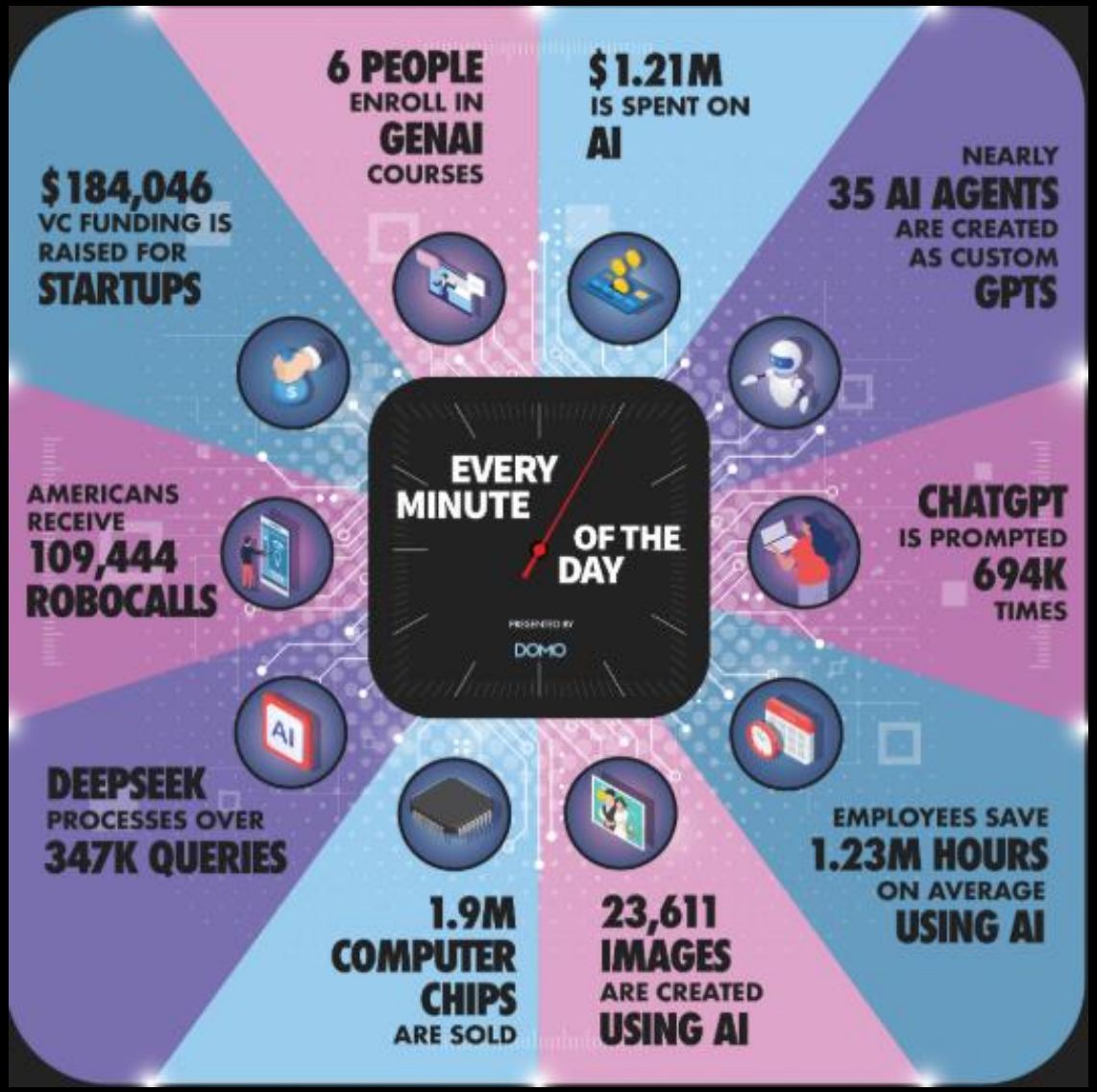
Hive Systems

Time it takes a hacker to brute force your password in 2025

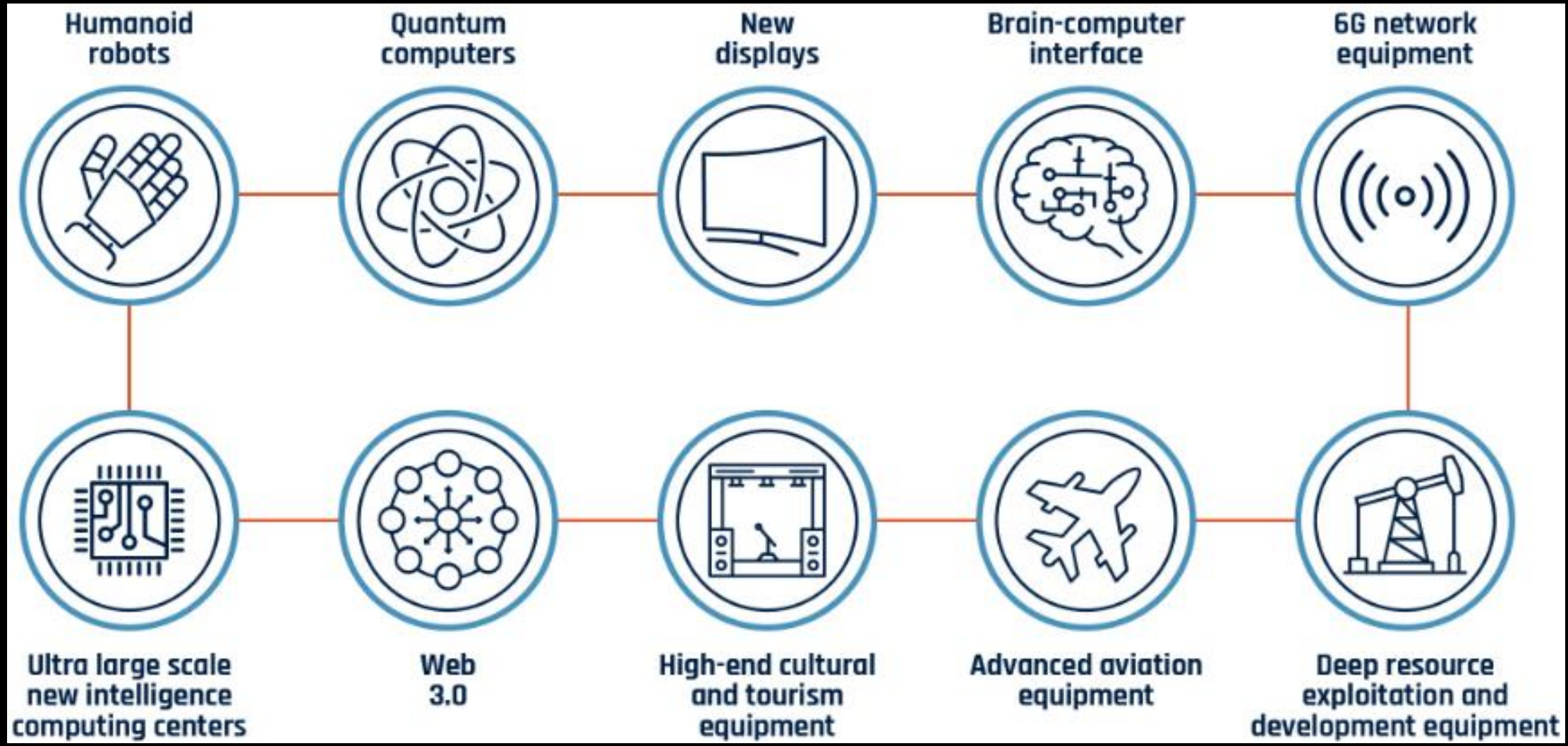
Hardware: 12 x RTX 5090
Password hash: bcrypt (10)

Read more and download at
hivesystems.com/password

Stats for AI

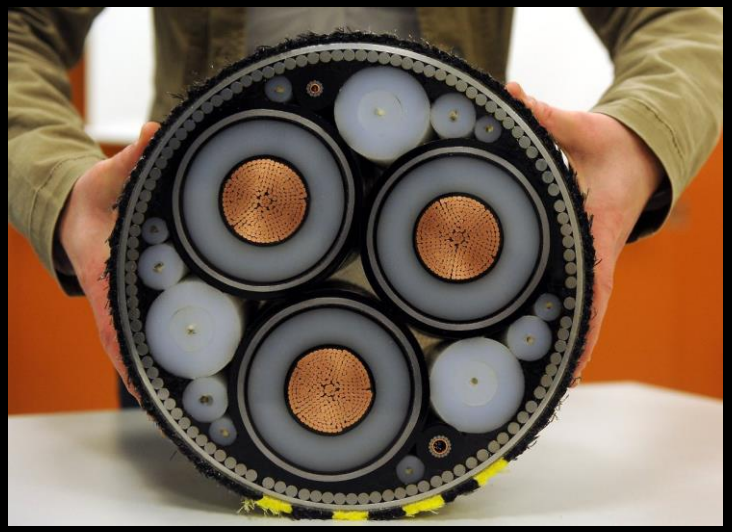


Example: Technology Priorities for PRC (China)

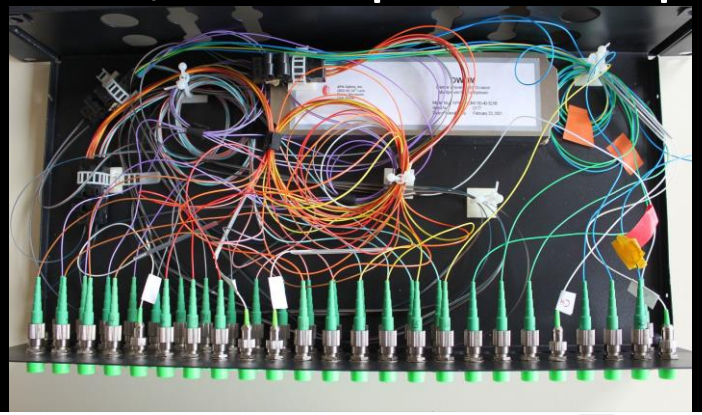


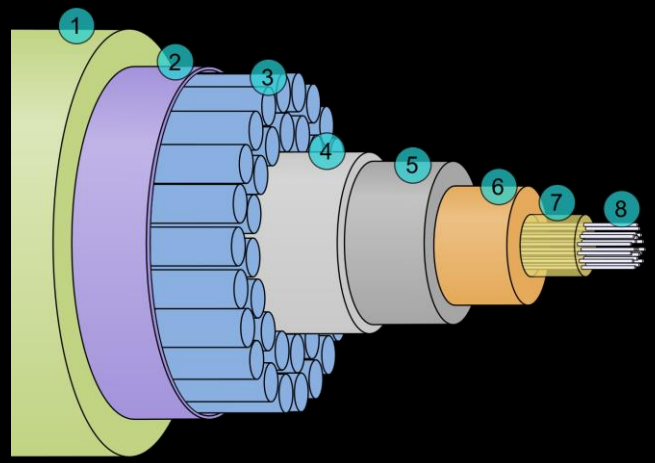
Undersea Cables

- Dense wavelength-division multiplexing (DWDM)
- 8-24 fibers per cable
- Modern is 80+ channels on a single fiber
- Each channel is up to 100Gbit/s



- Up to 192,000Gbps/192Tbps





A cross section of the shore-end of a modern submarine communications cable. 1 – Polyethylene 2 – Mylar tape 3 – Stranded steel wires 4 – Aluminium water barrier 5 – Polycarbonate 6 – Copper or aluminium tube 7 – Petroleum jelly 8 – Optical fibers